On linear completely regular codes with covering radius $\rho = 1$. Construction and classification[*]

J. Borges, J. Rifà,[†] V.A. Zinoviev[‡]

June 2, 2009

Abstract

Completely regular codes with covering radius $\rho = 1$ must have minimum distance $d \leq 3$. For $d = 3$, such codes are perfect and their parameters are well known. In this paper, the cases $d = 1$ and $d = 2$ are studied and completely characterized when the codes are linear. Moreover, it is proven that all these codes are completely transitive. **Keywords:** Linear completely regular codes, completely transitive codes, covering radius.

1 Introduction and Background

Let $\mathbb{F}_q = GF(q)$ be the Galois Field with q elements, where q is a prime power. $\mathbb{F}_q^n$ denotes the n-dimensional vector space over $\mathbb{F}_q$. The all-zero vector in $\mathbb{F}_q^n$ is denoted by $\mathbf{0}$. Let $\mathrm{wt}(\mathbf{v})$ denote the *Hamming weight* of a vector $\mathbf{v} \in \mathbb{F}_q$

[*] This work has been partially supported by the Spanish MICINN Grants MTM2006-03250, TSI2006-14005-C02-01 and PCI2006-A7-0616, the AGAUR grant 2008PIV00050 and also by the Russian fund of fundamental researches 06-01-00226.

[†] J. Borges and J. Rifà are with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (email: {joaquim.borges,josep.rifa}@autonoma.edu).

[‡] V.A. Zinoviev is with the Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 127994, Russia (e-mail: zinov@iitp.ru).

(i.e. the number of its nonzero positions), and $d(\mathbf{v},\mathbf{u}) = \mathrm{wt}(\mathbf{v}-\mathbf{u})$ denotes the *Hamming distance* between two vectors $\mathbf{v}$ and $\mathbf{u}$. Given $\mathbf{v} \in \mathbb{F}_q^n$, denote by *supp*$(\mathbf{v})$ the *support* of the vector $\mathbf{v}$, that is, the set of coordinate positions where $\mathbf{v}$ has nonzero entries. We say that a vector $\mathbf{u} = (u_1,\ldots,u_n) \in \mathbb{F}_q^n$ *covers* a vector $\mathbf{v} = (v_1,\ldots,v_n) \in \mathbb{F}_q^n$ if $v_i \neq 0$ implies $v_i = u_i$.

A q-ary *code* C of length n is a subset of $\mathbb{F}_q^n$. If C is a k-dimensional linear subspace of $\mathbb{F}_q^n$, then C is a *linear* code, denoted by $[n,k,d]_q$, where d is the *minimum distance* between any pair of codewords.

Let C be a q-ary code with minimum distance d, the *packing radius* of C is

$$e = \left\lfloor \frac{d-1}{2} \right\rfloor .$$

Such a code is said to be an e-*error-correcting* code.

Given any vector $\mathbf{v} \in \mathbb{F}_q^n$, its *distance* to the code C is

$$d(\mathbf{v}, C) = \min_{\mathbf{x}\in C}\{d(\mathbf{v},\mathbf{x})\}$$

and the *covering radius* of the code C is

$$\rho = \max_{\mathbf{v}\in\mathbb{F}_q^n}\{d(\mathbf{v},C)\}.$$

Clearly $e \leq \rho$ and C is said to be *perfect* when $e = \rho$.

For any $\mathbf{x} \in \mathbb{F}_q^n$, let $D = C + \mathbf{x}$ be a *translate* of C. The *weight* $\mathrm{wt}(D)$ of D is the minimum weight of the codewords of D.

Definition 1.1 *A q-ary code C is called* completely regular *if the weight distribution of any translate D of C is uniquely defined by the weight of D.*

Equivalently, C is completely regular if for all $\mathbf{x} \in \mathbb{F}_q^n$ such that $d(\mathbf{x}, C) = t$, the number of codewords at distance i $(0 \leq i \leq n)$ from $\mathbf{x}$ depends only on t and i.

Given a code C with covering radius ρ, let $C(\rho)$ be the set of vectors at distance ρ from C. The next statement can be found in [7] for binary codes. For the non-binary case it can be proven in similar way.

Lemma 1.2 *If a q-ary code C is completely regular with covering radius ρ, then $C(\rho)$ is also completely regular.*

A *linear automorphism* of $\mathbb{F}_q^n$ is a coordinate permutation together with a product by a nonzero scalar value at each position. Such an automorphism σ can be represented by a $n \times n$ monomial matrix M such that $\mathbf{x}M = \sigma(\mathbf{x})$, for all $\mathbf{x} \in \mathbb{F}_q^n$. From now on, if $C \subseteq \mathbb{F}_q^n$ is a linear code, the *full automorphism group* of C, denoted $\mathrm{Aut}(C)$, is the group of linear automorphisms of $\mathbb{F}_q^n$ that leaves C invariant. We say that $\mathrm{Aut}(C)$ is *transitive* if it is transitive when acts on the set of weight one vectors of $\mathbb{F}_q^n$.

Lemma 1.3 *Let $C, D \subseteq \mathbb{F}_q^n$ be two linear equivalent codes, i.e. there is a linear automorphism σ of $\mathbb{F}_q^n$ such that $D = \sigma(C)$. Then $\mathrm{Aut}(C)$ is transitive if and only if $\mathrm{Aut}(D)$ is transitive.*

Proof: Notice that for all $g \in \mathrm{Aut}(C)$, $\sigma g \sigma^{-1} \in \mathrm{Aut}(D)$. Assume that $\mathrm{Aut}(C)$ is transitive. Let $\mathbf{x}$ and $\mathbf{y}$ be weight one vectors, we want to find $\delta \in \mathrm{Aut}(D)$ such that $\delta(\mathbf{x}) = \mathbf{y}$. Let $\tau \in \mathrm{Aut}(C)$ such that $\tau(\sigma^{-1}(\mathbf{x})) = \sigma^{-1}(\mathbf{y})$, then $\sigma\tau\sigma^{-1}(\mathbf{x}) = \mathbf{y}$ and $\sigma\tau\sigma^{-1} \in \mathrm{Aut}(D)$. The statement then follows reversing the roles of C and D. ■

For a linear code C, the group $\mathrm{Aut}(C)$ acts on the set of cosets of C in the following way: for all $\phi \in \mathrm{Aut}(C)$ and for every vector $\mathbf{v} \in \mathbb{F}_q^n$ we have $\phi(\mathbf{v} + C) = \phi(\mathbf{v}) + C$.

In [5] and [10] the following definition has been given for the case of linear codes.

Definition 1.4 *Let C be a q-ary linear code with covering radius ρ. Then C is completely transitive if $\mathrm{Aut}(C)$ has $\rho + 1$ orbits when acts on the cosets of C.*

Since two cosets in the same orbit should have the same weight distribution, it is clear that any completely transitive code is completely regular. The following statement can be generalized for the case $\rho > 1$ replacing transitivity by ρ-homogeneity [10]. Here, we are only interested in the case $\rho = 1$.

Lemma 1.5 *Let C be a $[n,k,d]_q$ code with covering radius $\rho = 1$. If $\mathrm{Aut}(C)$ is transitive, then C is completely transitive.*

Proof: Obvious, since all cosets of C, different of C, have leaders of weight 1. Thus, all such cosets are in the same orbit. ■

It has been conjectured [7] for a long time that if C is a completely regular code and $|C| > 2$, then $e \leq 3$. For the special case of binary linear completely transitive codes [10], the problem of existence is solved: it is proven in [2, 3] that for $e \geq 4$ such nontrivial codes do not exist. The conjecture is also proven for the case of perfect codes ($e = \rho$) [12, 14] and quasi-perfect ($e+1 = \rho$) uniformly packed codes [6, 13], defined and studied also in [1, 11].

When $e \leq 3$, there are well known completely regular codes and, recently, we have presented new constructions of binary and non-binary completely regular codes [4, 8, 9]. However, there does not exist a general classification of completely regular codes with $e \leq 3$. In this paper we consider q-ary linear completely regular codes with $\rho = 1$. A surprising fact is that to characterize all linear completely regular codes with $\rho = 1$ we need only three constructions (q-repeated code construction, direct construction and Kronecker product construction).

The paper is organized as follows. In Section 2 we present the q times repeating construction to obtain linear or nonlinear q-ary completely regular codes with $d = 1$. In Section 3, we give a direct construction to obtain q-ary linear completely regular codes with $\rho = 1$ and $d \in \{1, 2\}$, we also introduce the Kronecker product of matrices as an important tool to characterize q-ary linear completely regular codes with $\rho = 1$ and, finally, we show that all such completely regular codes are completely transitive too.

2 Completely regular codes with $d = 1$ and the q-repeated code construction

We start with a first example of family of completely regular codes with minimum distance $d = 1$.

Lemma 2.1 *Let C be a perfect (binary or non-binary) code. Then $C(\rho)$ has minimum distance 1.*

Proof: Without loss of generality, we assume that $\mathbf{0} \in C$. Let $\mathbf{x} \in C(\rho)$ with $\mathrm{wt}(\mathbf{x}) = \rho$ and let $\mathbf{x}'$ be a vector such that $d(\mathbf{x}, \mathbf{x}') = 1$ and $\mathrm{wt}(\mathbf{x}') \geq \rho$. We claim that $\mathbf{x}' \in C(\rho)$ and then the minimum distance in $C(\rho)$ is 1. Assume to the contrary that $\mathbf{x}' \notin C(\rho)$, then clearly $d(\mathbf{x}', C) = \rho - 1$. Notice also that a codeword $\mathbf{y}$ at distance $\rho - 1$ of $\mathbf{x}'$ cannot be $\mathbf{0}$. Hence we obtain a contradiction because $\mathbf{x}$ is at distance ρ from more than one codeword. ■

As we have seen in Lemmas 1.2 and 2.1, the covering set $C(\rho)$ of any perfect code is a completely regular code with minimum distance $d = 1$. In particular, if C is a single error-correcting code ($e = 1$), then $C(\rho)$ is exactly the complement of C. But these are not the only examples of completely regular codes with $d = 1$.

Let C be a $[n, k, d]_q$ code. We construct the q-repeated code $C' \subseteq \mathbb{F}_q^{n+1}$ of C as follows: for any codeword $\mathbf{x} = (x_1, \ldots, x_n) \in C$, we have q codewords in C', namely

$$(0, x_1, \ldots, x_n), (1, x_1, \ldots, x_n), \ldots, (q - 1, x_1, \ldots, x_n).$$

Lemma 2.2 *Let C be a $[n, k, d]_q$ code and let $C' \subseteq \mathbb{F}_q^{n+1}$ be its q-repeated code. Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ be a vector at distance i from α_i codewords in C and at distance $i - 1$ from α_{i-1} codewords in C. Then, any vector of the form $\mathbf{x}' = (x_0, x_1, \ldots, x_n)$ is at distance i from exactly $\alpha_i + (q - 1)\alpha_{i-1}$ codewords in C'.*

Proof: For any codeword $\mathbf{z} = (z_1, \ldots, z_n) \in C$ such that $d(\mathbf{z}, \mathbf{x}) = i$ we have that $\mathbf{z}' = (x_0, z_1, \ldots, z_n)$ is in C' and $d(\mathbf{z}', \mathbf{x}') = i$. Moreover, for any codeword

$\mathbf{y} = (y_1, \ldots, y_n) \in C$ such that $d(\mathbf{y}, \mathbf{x}) = i - 1$, we have that the $q - 1$ vectors of the form $(y_0, y_1, \ldots, y_n)$ with $y_0 \neq x_0$ are codewords in C' and they are at distance i from $\mathbf{x}'$. It is clear that there are no more codewords in C' at distance i from $\mathbf{x}'$. ■

Theorem 2.3 (*q-Repeated code construction*) *Let C be a $[n, k, d]_q$ code with covering radius ρ. Then the q-repeated code $C' \subseteq \mathbb{F}_q^{n+1}$ has $\rho' = \rho$ and minimum distance $d' = 1$. Moreover C' is completely regular if and only if C is completely regular.*

Proof: For any vector $\mathbf{x}' = (x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1}$, call $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ the corresponding 'reduced' vector. Suppose that $\mathbf{y} = (y_1, \ldots, y_n) \in C$ is a codeword at minimum distance from $\mathbf{x}$. Then it is clear that $\mathbf{y}' = (x_0, y_1, \ldots, y_n)$ is a codeword in C' at minimum distance from $\mathbf{x}'$. Therefore $\rho = \rho'$.

Now, assume that C is completely regular. For any vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ at distance $t \leq \rho$ from C, define $\alpha_i(t)$ as the number of codewords in C at distance i from $\mathbf{x}$ $(0 \leq i \leq n)$. As C is completely regular, we know that $\alpha_i(t)$ does not depend on $\mathbf{x}$, but just on t and i. We want to see that for the vector $\mathbf{x}' = (x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1}$, which is at distance t form C', we also have that the number of codewords in C' at distance i, say $\alpha'_i(t)$, depends only on t and i. But this is straightforward because using Lemma 2.2 we have $\alpha'_i(t) = \alpha_i(t) + (q-1)\alpha_{i-1}(t)$, for all $i = 0, \ldots, n$, and $\alpha'_{n+1}(t) = (q-1)\alpha_n(t)$.

Conversely, assume that C is not completely regular. Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ be such that $d(\mathbf{x}, C) = d(\mathbf{y}, C) = t > 0$ and let $\alpha_{\mathbf{x},i}(t)$ (respectively $\alpha_{\mathbf{y},i}(t)$) denote the number of codewords at distance i from $\mathbf{x}$ (respect. $\mathbf{y}$), for $0 \leq i \leq n$. Since C is not completely regular, we can select $\mathbf{x}$ and $\mathbf{y}$ such that $\alpha_{\mathbf{x},i}(t) \neq \alpha_{\mathbf{y},i}(t)$ for some $i \geq t$. Let i be the minimum possible such value (possibly, $i = t$), that is $\alpha_{\mathbf{x},i-1}(t) = \alpha_{\mathbf{y},i-1}(t)$. Then, for the q-repeated vectors $\mathbf{x}'$ and $\mathbf{y}'$, we have $\alpha'_{\mathbf{x}',i}(t) \neq \alpha_{\mathbf{y}',i}(t)$ by Lemma 2.2. Consequently, C' is not completely regular. ■

Hence, we can start with any completely regular code and obtain an infinite family of completely regular codes with the same covering radius. We remark that this construction is also valid for nonlinear codes.

Conversely, for the linear case with $d = 1$, we have the following:

Corollary 2.4 *Let $C \neq \mathbb{F}_q^n$ be a q-ary linear code with minimum distance $d = 1$ and covering radius ρ. Then C can be obtained using the q-repeated code construction (repeating the process some number of times) from a code D which has minimum distance greater than one and covering radius ρ. Moreover, C is completely regular if and only if D is completely regular.*

Proof: Let G be a generator matrix for C containing all linear independent codewords of weight 1. The desired code D is then obtained removing from G all row vectors of weight 1 and the resulting zero columns. As we have seen in Theorem 2.3, the covering radius does not change and C is completely regular if and only if D is completely regular. ■

3 Completely regular codes with $\rho = 1$

Since $e \leq \rho$, completely regular codes with $\rho = 1$ must have minimum distance $d \leq 3$. When $d = 1$ we have seen, in the previous section, that we can obtain these codes using the q-repeated construction starting from codes with the same covering radius $\rho = 1$ and with minimum distance greater than 1. For $d = 3$, we have $e = \rho$ and these codes are perfect. Linear perfect codes with $e = 1$ are the well known Hamming codes.

Therefore, if $\rho = 1$ the case to focus our interest is $d = 2$. A first example where we construct linear codes with these parameters, $\rho = 1$ and $d = 2$, is given by the following theorem.

Theorem 3.1 (*Direct construction*) *Let C be a $[m+1, m, d]_q$ code defined by a generating matrix G,*

$$G \ = \ [I|\mathbf{h}],$$

where I is the identity matrix of order m, and $\mathbf{h}$ is an arbitrary nonzero column vector from $\mathbb{F}_q^m$. Then, if $\mathrm{wt}(\mathbf{h}) < m$, the code C is a completely regular code *with $d = \rho = 1$. If* $\mathrm{wt}(\mathbf{h}) = m$*, then C is a completely regular code with $d = 2$ and $\rho = 1$.*

Proof: Clearly, if $\mathrm{wt}(\mathbf{h}) < m$, then the minimum distance of C is 1 and if $\mathrm{wt}(\mathbf{h}) = m$, then the minimum distance is 2. A parity check matrix for C is given by

$$H = [-\mathbf{h}^t|1]$$

and any pair of columns are linearly dependent. Hence $\rho = 1$.

In order to see that C is completely regular, we take a vector $\mathbf{x}$ at distance 1 from C (or, the same, $\mathbf{x} \notin C$) and we prove that the number of codewords at distance 1 from $\mathbf{x}$ is always the same. Assume, without loss of generality, that $\mathbf{x} = (x_1, \ldots, x_{m+1})$ has weight 1. Let $w = \mathrm{wt}(\mathbf{h})$ and let x_i be the nonzero coordinate of $\mathbf{x}$. First, we consider the case $i < m+1$. The codewords at distance 1 from $\mathbf{x}$ are $\mathbf{0}$, $x_i\mathbf{v}^{(i)}$, where $\mathbf{v}^{(i)}$ is the i-th row of G (notice that $\mathbf{v}^{(i)}$ has weight 2, otherwise $\mathbf{x}$ would be a codeword) and the codewords of weight 2 with the value x_i at the i-th coordinate which are of the form: $\mathbf{y}^{(ij)} = x_i\mathbf{v}^{(i)} + \alpha_j\mathbf{v}^{(j)}$ for all row vectors $\mathbf{v}^{(j)}$ of weight 2 ($j \neq i$), where $\alpha_j \in \mathbb{F}_q$ is taken such that the last coordinate of $\mathbf{y}^{(ij)}$ is zero. Thus, we have $w + 1$ codewords at distance 1 from $\mathbf{x}$. Finally, consider the case $i = m + 1$. The codewords at distance 1 from $\mathbf{x}$ are $\mathbf{0}$ and the w codewords of the form $\mathbf{y}^{(j)} = \alpha_j\mathbf{v}^{(j)}$, where $\mathbf{v}^{(j)}$ has weight 2 and $\alpha_j \in \mathbb{F}_q$ is taken such that the last coordinate of $\mathbf{y}^{(j)}$ is x_i. Again, we obtain $w + 1$ codewords at distance 1 from $\mathbf{x}$. ■

From now on, our goal is to classify all the linear completely regular codes with $\rho = 1$ and $d = 2$.

We will begin by introducing the Kronecker product of matrices and showing that this tool will help us in the construction of linear completely regular codes with the required parameters.

Definition 3.2 *The Kronecker product of two matrices $A = [a_{r,s}]$ and $B = [b_{i,j}]$ over $\mathbb{F}_q$ is a new matrix $H = A \otimes B$ obtained by changing any element $a_{r,s}$ in A by the matrix $a_{r,s}B$.*

A *repetition code* is a $[n,1,n]_q$ code. In this paper, we assume that such a repetition code has all codewords of the form $(c,c,\dots,c)$ for $c \in \mathbb{F}_q$.

Lemma 3.3 *Let $\mathcal{H}$ be $[n,k,3]_q$ Hamming code. Then, $\mathrm{Aut}(\mathcal{H})$ is transitive.*

Proof: Let G and H be generator and parity check matrices, respectively, for $\mathcal{H}$. Let $\mathbf{x}$ and $\mathbf{y}$ be an arbitrary pair of weight one vectors. We want to find a linear automorphism of $\mathcal{H}$ that sends $\mathbf{x}$ to $\mathbf{y}$. It is straightforward to find an invertible $(n-k)\times(n-k)$ matrix K, with entries in $\mathbb{F}_q$ and such that $KH\mathbf{x}^t = H\mathbf{y}^t$. Since H is a parity check matrix of a Hamming code, there exists a monomial $n \times n$ matrix M such that $KH = HM^t$. Since $H(M^tG^t) = KHG^t = 0$, we have that GM is also a generator matrix for $\mathcal{H}$. Thus, M is the monomial matrix associated to a linear automorphism $\phi \in \mathrm{Aut}(\mathcal{H})$.

Now, $KH\mathbf{x}^t = H\mathbf{y}^t$ implies $HM^t\mathbf{x}^t = H\mathbf{y}^t$. As $M^t\mathbf{x}^t$ and $\mathbf{y}^t$ have weight one and H has no repeated columns, we conclude $\mathbf{x}M = \mathbf{y}$ or, the same, $\phi(\mathbf{x}) = \mathbf{y}$. ■

Theorem 3.4 *Let C be the linear code over $\mathbb{F}_q$ which has $H = A \otimes B$ as a parity check matrix, where A is a generator matrix for the repetition $[n_a,1,n_a]_q$ code of length n_a and B is a parity check matrix of a Hamming code with parameters $[n_b,k_b,3]_q$, where $n_b = (q^{m_b}-1)/(q-1)$ and $k_b = n_b - m_b$.*

(i) Code C has length $n = n_a \cdot n_b$, dimension $k = n - m_b$ and covering radius $\rho = 1$.

(ii) If $n_a > 1$, then the minimum distance of C is $d = 2$. If $n_a = 1$, then $d = 3$.

(iii) $\mathrm{Aut}(C)$ is transitive and, therefore, C is a completely transitive code and a completely regular code.

Proof: It is straightforward to check that the code C has length $n = n_a \cdot n_b$, dimension $k = n - m_b$ and covering radius $\rho = 1$.

If $n_a = 1$, then C is a Hamming code and $d = 3$. If $n_a > 1$, then H has repeated columns and $d = 2$.

The matrix H is of the form

$$H = [B\ B\ \cdots B],$$

where B is a parity check matrix for a Hamming code $\mathcal{H}$. By Lemma 3.3, $\mathrm{Aut}(\mathcal{H})$ is transitive on the set of weight one vectors with support contained in the set of coordinate positions of $\mathcal{H}$. Hence we have that $\mathrm{Aut}(C)$ is transitive on each set of weight one vectors with support contained in the set of n_b coordinate positions corresponding to each submatrix B. Now consider two vectors of weight one $\mathbf{x} \in \mathbb{F}_q^n$ and $\mathbf{y} \in \mathbb{F}_q^n$, such that the nonzero entry of $\mathbf{x}$ is $x \in \mathbb{F}_q$ at position i and the nonzero entry of $\mathbf{y}$ is y at position j and assume that i and j are in different n_b-sets, i.e. sets of cardinality n_b, of coordinate positions. Let $\varphi \in \mathrm{Aut}(C)$ such that $\varphi(\mathbf{x}) = \mathbf{x}'$, where $\mathbf{x}'$ has weight one with its nonzero entry equal to y at position i', in the same n_b-set of coordinate positions, where the column vector of H in position i' is the same that the column vector in position j. Clearly, the transposition $\tau = (i', j)$ is a linear automorphism of C. Thus, $\tau(\varphi(\mathbf{x})) = \mathbf{y}$.

Therefore, we have proven that $\mathrm{Aut}(C)$ is transitive and, by Lemma 1.5, C is a completely transitive code and hence a completely regular code.

■

The following step is to prove that, vice versa, codes constructed in Theorem 3.4 are the unique linear completely regular codes with $d = 2$ and $\rho = 1$.

Lemma 3.5 *Let C be a completely regular $[n, k, 2]_q$ code with covering radius $\rho = 1$. Let n_a be the number of codewords at distance 1 from any vector $\mathbf{x} \notin C$. Then the following statements are equivalent:*

(i) For any pair of coordinate positions i and j, there exists a codeword of weight 2 with support $\{i, j\}$.

(ii) $n_a = n$.

(iii) C is a q-ary part of the whole space, i.e. $|C| = q^{n-1}$.

(iv) Code C has a generator matrix of the form

$$G = [I|\mathbf{h}],$$

where I is the identity matrix of order $n-1$, and $\mathbf{h}$ is a column vector of weight $n-1$ from $\mathbb{F}_q^{n-1}$.

(v) Dual code of C is equivalent to a repetition $[n,1,n]_q$ code.

Proof: Let $\mathbf{x} \notin C$, without loss of generality we assume that $\mathbf{x}$ has weight 1 and let x_i be the nonzero coordinate of $\mathbf{x}$. Then the codewords at distance 1 from $\mathbf{x}$ are the all-zero codeword and all codewords of weight 2 with x_i at the i-th coordinate. Such codewords have the remaining nonzero coordinate in different places (otherwise C would have codewords of weight one). There are $n-1$ possible different places. Hence (i) and (ii) are equivalent.

Define the following simple bipartite graph with vertices which are all points of $\mathbb{F}_q^n$ and with edges, connecting the points of C with the points $C(\rho) = \mathbb{F}_q^n \setminus C$, if these two points are at distance one from each other. Count the number of edges in two ways. From one side, any codeword of C is at distance 1 from $(q-1)n$ points of $C(\rho)$. From the other side, any point of $C(\rho)$ is at distance 1 from n_a points of C. Since these numbers should be equal, we conclude that

$$n(q-1)\,|C| \;=\; n_a\,|\mathbb{F}_q^n \setminus C|,$$

which gives

$$(q-1)n = (q^{n-k}-1)n_a, \tag{1}$$

where k is the dimension of C. It is clear that $n_a = n$ if and only if $k = n-1$. This gives the equivalence between (ii) and (iii).

The equivalence between (iii) and (iv), and between (iv) and (v) are trivial. ■

Lemma 3.6 *Let C be a completely regular $[n,k,2]_q$ code with covering radius $\rho = 1$. Let n_a be the number of codewords at distance one from any vector not in C. If $k < n-1$, then the set of coordinate positions $\{1,\ldots,n\}$ can be partitioned into n_a-sets, $X_1,\ldots,X_{n/n_a}$, such that any codeword of weight 2 has its support contained in one of these sets.*

Proof: First note that $n_a \geq 2$, otherwise C would be a perfect code with $d = 2$ which does not exist. By Lemma 3.5, since $k < n-1$, we also have $n_a < n$ and clearly n_a divides n by (1).

Now, for any vector $\mathbf{u} \notin C$ of weight 1, consider the union of the supports of the $n_a - 1$ codewords of weight 2 that cover $\mathbf{u}$. Denote by $X(\mathbf{u})$ such set of coordinate positions and note that $|X(\mathbf{u})| = n_a$. Let $\mathbf{v}$ be another vector of weight 1 such that its support is not in $X(\mathbf{u})$. It suffices to prove that $X(\mathbf{u})$ and $X(\mathbf{v})$ are disjoin sets. Assume to the contrary that a coordinate position i belongs to $X(\mathbf{u}) \cap X(\mathbf{v})$. This means that there is a codeword $\mathbf{x}$ of weight 2 covering $\mathbf{u}$ and a codeword $\mathbf{y}$ of weight 2 covering $\mathbf{v}$ and $supp(\mathbf{x}) \cap supp(\mathbf{y}) = \{i\}$. Let $\mathbf{y}'$ be a multiple of $\mathbf{y}$ such that $y'_i = x_i$. Then, the codeword $\mathbf{z} = \mathbf{x} - \mathbf{y}'$ covers $\mathbf{u}$ but $supp(\mathbf{z}) \nsubseteq X(\mathbf{u})$ which is a contradiction. ■

Corollary 3.7 *With the same hypothesis of Lemma 3.6, let D_i be the code that has the codewords of C such that their supports are contained in X_i and deleting the coordinate positions outside of X_i. Then, D_i is a linear completely regular code of length n_a, dimension $n_a - 1$, minimum distance $d = 2$, and covering radius $\rho = 1$. A generator matrix for D_i is:*

$$G_i = [I|\mathbf{h}],$$

where $\mathbf{h}$ is a column vector of weight $n_a - 1$.

Proof: For any $i = 1, \ldots, n/n_a$, it is straightforward to see that D_i is a linear code of length n_a and minimum distance $d = 2$. Moreover, let Z be the set of weight two codewords covering some fixed vector of weight one. Then Z is a set of $n_a - 1$ linear independent codewords. Thus, by Theorem 3.1, code D_i is completely regular with $\rho = 1$. ■

Now, it is clear that any linear completely regular code C with $d = 2$ and $\rho = 1$ can be 'decomposed' into completely regular codes D_i of type 'direct construction'. In order to complete the classification we need the following technical results.

Lemma 3.8 *With the same hypothesis as in Lemma 3.6, let* $\mathbf{x} = (x_1, \ldots, x_n) \in C$ *and let* X_j *be one of the sets as in Lemma 3.6, such that* $supp(\mathbf{x}) \cap X_j \neq \emptyset$*. Then there exists a codeword* $\mathbf{x}' = (x'_1 \ldots, x'_n) \in C$ *which coincides with* $\mathbf{x}$ *in all positions outside of* X_j*, such that* $|supp(\mathbf{x}') \cap X_j| \leq 1$*, and where for the case* $|supp(\mathbf{x}') \cap X_j| = 1$*, the nonzero element of* $\mathbf{x}'$ *occur in any position of* X_j*, i.e. for any* $i_j \in X_j$ *there is a such vector* $\mathbf{x}'$ *with nonzero element in position* i_j*.*

Proof: Let $\mathbf{x} = (x_1, \ldots, x_n) \in C$ and let X_j be such that $supp(\mathbf{x}) \cap X_j \neq \emptyset$. Now, adding codewords of weight 2 with support only in X_j (see Lemma 3.6), from $\mathbf{x}$ we easily arrive to $\mathbf{x}'$, which has either all zero coordinates on X_j, or exactly one nonzero coordinate which might be placed on any position of X_j. ■

Proposition 3.9 *With the same hypothesis as in Lemma 3.6, for each* $j = 1, \ldots, n/n_a$*, take and fix a coordinate position* $i_j \in X_j$*. Let* D' *be the code that has all codewords in* C *having their supports contained in* $I = \{i_1, \ldots, i_{n/n_a}\}$*. Let* D *be the code obtained from* D' *by deleting all coordinates outside of* I*. Then* $n/n_a \geq 3$ *and* D *is a Hamming code of length* n/n_a*.*

Proof: Clearly D is a linear code of length n/n_a. By Lemma 3.6, since we are assuming $k < n - 1$, D is not empty and the minimum weight of D is 3. Thus, we only need to prove that the covering radius of D is 1. Otherwise, assume that $\mathbf{v}$ is a vector (with coordinates in I) at distance 2 from D. Without loss of generality, we can assume that $\mathbf{v}$ has weight 2 with $supp(\mathbf{v}) = \{i_r, i_s\}$, $(i_r \in X_r, i_s \in X_s, r \neq s)$. The covering radius of C is $\rho = 1$, so we can take $\mathbf{x} \in C$ at distance one from $\mathbf{v}'$, where $\mathbf{v}'$ is the extension of vector $\mathbf{v}$ adding zeroes in all coordinate positions of $\{1, \ldots, n\} \backslash I$. By Lemma 3.6, $\mathbf{x}$ cannot have neither weight 2 nor weight 1, since the minimum distance of C is 2. Thus, $\mathbf{x}$ is a codeword of weight 3 with $supp(\mathbf{x}) = \{i_r, i_s, i\}$. Note that i cannot be in X_r or X_s, otherwise, using Lemma 3.8 we could obtain a codeword of weight 2 with support $\{i_r, i_s\}$, contradicting Lemma 3.6. We conclude that $n/n_a \geq 3$. Let $i \in X_t$, where $r \neq t \neq s$. Again, using Lemma 3.8, we can obtain a codeword

$\mathbf{x}' \in C$ such that $supp(\mathbf{x}') = \{i_r, i_s, i_t\}$, $x'_{i_r} = x_{i_r}$ and $x'_{i_s} = x_{i_s}$. Clearly, $\mathbf{x}'$ restricted to the I coordinates is a codeword in D of weight 3 and covers $\mathbf{v}$. Therefore $\mathbf{v}$ is not at distance 2 from D. ■

Corollary 3.10 *Let C be a $[n,k,2]_q$ completely regular code with covering radius $\rho = 1$ and let n_a be the number of codewords at distance one from any vector not in C. Then, either $n_a = n$, $k = n-1$ and C has generator matrix:*

$$G = [G_1];$$

or C has generator matrix:

$$G = \left[\begin{array}{ccc} G_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & G_{n/n_a} \\ \hline M_1 & \cdots & M_{n/n_a} \end{array} \right], \tag{2}$$

where G_i is a generator matrix of a $[n_a, n_a - 1, 2]_q$ code (which is completely regular) for all $i = 1, \ldots, n/n_a$, and M_i has $n_a - 1$ zero columns and one column $\mathbf{h}_i$ such that

$$\left[\begin{array}{ccc} \mathbf{h}_1 & \cdots & \mathbf{h}_{n/n_a} \end{array} \right]$$

is a generator matrix of a Hamming code $\mathcal{H}$.

Proof: We have already seen in Theorem 3.1 the case $n_a = n$, $k = n-1$.

Now, let $n_a < n$. By Corollary 3.7 and Proposition 3.9, it is clear that code C' generated by G is a subcode of C. But, the number of rows (which are all linear independent) of G is:

$$\frac{n}{n_a} \cdot (n_a - 1) + dim(\mathcal{H}).$$

Since (1), the length of $\mathcal{H}$ is

$$\frac{n}{n_a} = \frac{q^{n-k} - 1}{q - 1},$$

the dimension of $\mathcal{H}$ is $(n/n_a) - (n-k)$. Therefore

$$dim(C') = \frac{n}{n_a} \cdot (n_a - 1) + \frac{n}{n_a} - n + k = k.$$

Hence, $dim(C') = dim(C)$ and consequently $C' = C$. ■

Proposition 3.11 *Let C be a $[n,k,2]_q$ completely regular code with covering radius $\rho = 1$. Let n_a be the number of codewords at distance one from any vector not in C. Let A be a generator matrix of a repetition $[n_a, 1, n_a]$-code and let B be a parity check matrix for a Hamming q-ary code of length $n_b = n/n_a$.*

(i) If $k = n-1$, then code C is equivalent to a code with parity check matrix $H = A$.

(ii) If $k < n-1$, then C is equivalent to a code with parity check matrix $H = A \otimes B$.

Proof: If $k = n-1$, by Corollary 3.10, code C is given by a generator matrix of a $[n_a, n_a-1, 2]_q$ code. A parity check matrix for an equivalent code to C is the generator matrix of a repetition $[n_a, 1, n_a]$-code.

If $k < n-1$, we can start with a generator matrix as in (2). Then, we multiply the first $n_a(n_a-1)$ rows by appropriate values. After, we can multiply the columns to obtain the following generator matrix:

$$G = \left[\begin{array}{ccc} G' & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & G' \\ \hline M_1 & \cdots & M_{n/n_a} \end{array}\right], \tag{3}$$

where G' is a $(n_a-1) \times n_a$ matrix

$$G' \;=\; [I|\mathbf{h}].$$

Up to equivalence, we can assume that $\mathbf{h}$ has the value $q-1$ in all its entries and $M_1, \ldots, M_{n/n_a}$ are as in Corollary 3.10. We also assume that the nonzero column of each M_i is the first one.

Finally, we can permute the columns of the matrix

$$H = [B\ B\ \cdots\ B]$$

to obtain the matrix

$$H' = [B_1\ B_2\ \cdots\ B_{n/n_a}],$$

where B_i has all its columns equal to the i-th column of B. It is straightforward to see that G and H' are orthogonal matrices. ■

Finally, we summarize the main result of this paper.

Theorem 3.12 *Let C be a $[n,k,d]_q$ completely regular code with covering radius $\rho = 1$. Let A be a generator matrix for the repetition $[n_a, 1, n_a]_q$ code of length n_a and let B be a parity check matrix of a Hamming code with parameters $[n_b, k_b, 3]_q$, where $n = n_a n_b$, $n_b = (q^{m_b} - 1)/(q-1)$, $k_b = n_b - m_b$.*

(i) If $d = 1$, then C is the q-repeated code of a completely regular code C' with covering radius $\rho' = 1$ and minimum distance $d' \in \{1, 2\}$.

(ii) If $d = 2$, then $n_a > 1$ and C is equivalent to a code with parity check matrix $H = A$ or $H = A \oplus B$.

(iii) If $d = 3$, then $n_a = 1$ and C is a Hamming code and $H = B$ is a parity check matrix for C.

(iv) C is a completely transitive code.

Proof: We know that $d \in \{1, 2, 3\}$. We separate these three cases:

(i) We have proven this statement in Corollary 2.4.

(ii) This is proven in Proposition 3.11.

(iii) Obvious, since C is a perfect code.

(iv) If $d \in \{2, 3\}$, by Proposition 3.11 and Theorem 3.4, C is equivalent to a code C' such that $\mathrm{Aut}(C')$ is transitive. Thus, by Lemma 1.3, $\mathrm{Aut}(C)$ is transitive and, by Lemma 1.5, C is completely transitive.

If $d = 1$, then let D be the 'reduced' code, that is, the code obtained from C by doing the reverse operation of the q-repeated code construction. Since the covering radius of C and D is 1, we have that $C \neq \mathbb{F}_q^n$ and D is a completely regular code with $d > 1$ by Theorem 2.3. Therefore D is a completely transitive code. This means that we can choose a set of

$q^{n-k}-1$ coset leaders of weight one such that they are in the same orbit of $\mathrm{Aut}(D)$. But C has the same number of cosets and we can choose the same coset leaders. Since, clearly, $\mathrm{Aut}(D) \subseteq \mathrm{Aut}(C)$, we have that these coset leaders are in the same orbit. Therefore, all cosets different of C are in the same orbit and C is a completely transitive code.

■

References

[1] L.A. Bassalygo, G.V. Zaitsev & V.A. Zinoviev, "Uniformly packed codes," *Problems Inform. Transmiss.,* vol. 10, no. 1, pp. 9-14, 1974.

[2] J. Borges, & J. Rifa, "On the Nonexistence of Completely Transitive Codes", *IEEE Trans. on Information Theory*, vol. 46, no. 1, pp. 279-280, 2000.

[3] J. Borges, J. Rifa & V.A. Zinoviev "Nonexistence of Completely Transitive Codes with Error-Correcting Capability $e > 3$", *IEEE Trans. on Information Theory*, vol. 47, no. 4, pp. 1619-1621, 2001.

[4] J. Borges, J. Rifa & V.A. Zinoviev, "On non-antipodal binary completely regular codes", *Discrete Mathematics*, 2008, vol. 308, 3508 - 3525.

[5] M. Giudici, C.E. Praeger, "Completely Transitive Codes in Hamming Graphs", Europ. J. Combinatorics 20, pp. 647662, 1999.

[6] J.M. Goethals & H.C.A. Van Tilborg, "Uniformly packed codes," *Philips Res.*, vol. 30, pp. 9-36, 1975.

[7] A. Neumaier, "Completely regular codes," *Discrete Maths.*, vol. 106/107, pp. 335-360, 1992.

[8] J. Rifa & V.A. Zinoviev, "On new completely regular q-ary codes", *Problems of Information Transmission*, vol. 43, No. 2, 2007, 97 - 112.

[9] J. Rifa & V.A. Zinoviev, ”New completely regular q-ary codes, based on Kronecker products”, IEEE Transactions on Information Theory, 2009, to appear.

[10] P. Solé, “Completely Regular Codes and Completely Transitive Codes,” *Discrete Maths.*, vol. 81, pp. 193-201, 1990.

[11] N.V. Semakov, V.A. Zinoviev & G.V. Zaitsev, “Uniformly packed codes,” *Problems Inform. Transmiss.*, vol. 7, no. 1, pp. 38-50, 1971.

[12] A. Tietäväinen, “On the non-existence of perfect codes over finite fields,” *SIAM J. Appl. Math.*, vol. 24, pp. 88-96, 1973.

[13] H.C.A. Van Tilborg, *Uniformly packed codes.* Ph.D. Eindhoven Univ. of Tech., 1976.

[14] V.A. Zinoviev & V.K. Leontiev, “The nonexistence of perfect codes over Galois fields,” *Problems of Control and Information Th.*, vol. 2, no. 2, pp. 16-24, 1973.